Reclamation Manual

Directives and Standards

TEMPORARY RELEASE

(Expires 03/30/2016)

Configuration Management Documentation

1. **Introduction.** This document describes general requirements for documentation that must be reviewed and updated under configuration management control. Documentation that must be maintained per the configuration management process will be placed in three categories which include: design or guidance documents, procedure or process documents, and configuration documents. Design or guidance documents describe system hardware, software, and their interfaces for cyber assets subject to the NERC CIP Reliability Standards. Design documents may be provided by Supervisory Control and Data Acquisition (SCADA) system or Physical Access Control System (PACS) suppliers and suppliers of SCADA system or PACS modules, but the documentation package must be updated when system changes are made. Procedure documents describe methods which may include software or hardware updates, revisions, recovery, and test procedures. Configuration documents describe settings for hardware, software, and interface points that are necessary to provide functionality and security features for a particular installation. Required documentation may be system-generated (as in group policy reports, etc.) or documentation may take the form of user generated hard copies. For audit purposes, sites must be prepared to generate and present the required documentation upon request.

2. **Design Documents.** Design or guidance documentation will generally include a large multi-volume set of data. In general, the following documentation must be provided:

   A. **Hardware Documentation.** System hardware must be described, and must include the following, at a minimum:

      (1) An inventory of all cyber assets with processes to identify the subset of Critical Cyber Assets must be provided. See the Reclamation Manual Temporary Reclamation Manual Release (TRMR) D&S, *Critical Cyber Asset (CCA) Identification Supporting North American Electric Reliability Corporation (NERC) Reliability Standard Compliance* (IRM TRMR-34), for additional information. This list must be reviewed annually.

      (2) A list of changes for cyber assets subject to the NERC CIP Reliability Standards including: additions, deletions, and revisions must be maintained pursuant to CIP-007, R9.

   B. **Software Documentation.** System software for cyber assets subject to the NERC CIP Reliability Standards must be described. This must include designs for application software, communication system software, all software associated with operator interface systems, and all software development systems.

3. **Procedure Documents.** A wide variety of procedures must be documented to provide control of hardware and software maintenance activities. The list of documents provided is a general list and unique procedures associated with a particular set of cyber equipment must be developed as required.

   A. **Configuration Management Plan (CMP).** The CMP documentation as identified in this D&S and (CIP-003, R6).

   B. **CCA Access Procedures.** Organizational and technical procedures need to be developed to document controls used to secure access to all cyber assets subject to the NERC CIP Reliability Standards (CIP-007, R5).

   C. **Update Procedures.** Procedures must be developed to maintain control over updates that are performed to all cyber assets subject to the NERC CIP Reliability Standards. Patch management, virus/malware update, and all other system update (vendor supplied software, etc.) methods must be described in written procedures (CIP-007, R3, R4).

   D. **Test Procedures.** Test procedures must be developed to verify security controls are functioning properly when significant system changes are made. Depending on the nature of the change, these procedures include: ESP Vulnerability tests (CIP-005, R4), Cyber Vulnerability tests (CIP-007, R8), General Test Procedures (CIP-007, R1), and Ports and Impact Analysis Testing (CIP-007, R2).

   E. **Local Incident Response Procedures and Recovery Plans.** If local incident response procedures are developed, those procedures must be maintained per configuration management processes when a significant change to cyber assets subject to the NERC CIP Reliability Standards forces a revision to the incident procedures (CIP-008). Local recovery plans will be required for each cyber asset subject to the NERC CIP Reliability Standards. Test procedures for testing backup media must also be provided (CIP-009).

4. **Configuration Documents.** Configuration documents that must be placed under configuration management processes are included in the following list.

   A. **Baseline Ports and Services.** A configuration baseline for unused ports and services must be determined (see *Appendix A*, *Ports and Impact Analysis Testing).* The baseline will be used for testing purposes to verify security controls have not been compromised when system changes are made (CIP-007, R2).

B. **Minimum Password Complexity Configuration Settings.** Minimum password complexity setting must be documented to verify password complexity requirements. (For additional clarification refer to the D&S.)

C. **Shared Account Privileges.** Shared accounts must be documented and revised as necessary to verify required security controls are being maintained (CIP-007, R5.2).

D. **Access Control.** Configuration settings for all logical access settings to ESP access points and all CCA must be documented (CIP-005, R2; CIP-007, R5).